Docket No.   AUS920000797US1

CLAIMS:

What is claimed is:

5   1.   A method in a data processing system for managing
access to data in a keystore, the method comprising:
        receiving a request for access to an item of data
from a requestor, wherein the item of data is encrypted
using a key;
10   determining whether the requestor is a trusted
requestor;
        responsive to a determination that the requestor is
a trusted requestor, decrypting the item of data using
the key to form a decrypted item of data; and
15   sending the decrypted item of data to the requestor.

2.   The method of claim 1, wherein the requestor is an
application.

20   3.   The method of claim 1, wherein the Keystore is a
Java Keystore.

4.   The method of claim 1, wherein the item of data is
another key.
25

5.   The method of claim 1, wherein the item of data is a
certificate.

6.   The method of claim 1, wherein the item of data is
30   indexed within the Keystore using an alias.

Docket No. AUS920000797US1

7. The method claim 6, wherein the request includes the alias further comprising:

    responsive to an absence of a determination that the requestor is a trusted requestor, returning a null result
5   to the requestor.

8. The method of claim 1 further comprising:

    responsive to receiving a request to add a new item of data to the Keystore, encrypting the new item of data
10 to form an encrypted item of data; and

    storing the encrypted item of data in the Keystore.

9. The method of claim 8 further comprising:

    storing the new item of data in the Keystore.
15

10. The method of claim 8, wherein each item of data in the Keystore is associated with an alias.

11. A method in a data processing system for managing
20 access to data in a keystore, the method comprising:

    receiving a request for access to an item of data from a requestor, wherein the item of data is encrypted using a key;

    determining whether the requestor is a trusted
25 requestor; and

    responsive to a determination that the requestor is a trusted requestor, sending the key and the item of data to the requestor.

30 12. A Keystore system comprising:

    a Keystore object including:

Docket No.   AUS920000797US1

a key; and

a plurality of entries, wherein each entry within
the plurality of entries is encrypted using the key;
and

5   a Keystore process, wherein the Keystore process
provides access to the plurality of entries in response
to a request from a trusted application by providing the
key to the trusted application.

10   13.   The Keystore system of claim 12, wherein the
plurality of entries is indexed using a plurality of
aliases and wherein the request includes an alias for a
requested entry.

15   14.   The Keystore system of claim 12, wherein the
plurality of entries is a first plurality of entries and
wherein the Keystore object includes a second plurality
of entries corresponding to the first plurality of
entries in an unencrypted form.
20

15.   A data processing system comprising:
a bus system;
a communications unit connected to the bus, wherein
data is sent and received using the communications unit;
25   a memory connected to the bus system, wherein a set
of instructions are located in the memory; and
a processor unit connected to the bus system,
wherein the processor unit executes the set of
instructions to receive a request for access to an item
30   of data from a requestor, wherein the item of data is
encrypted using a key, determine whether the requestor is

a trusted requestor, and send the key and the item of
data to the requestor, in response to a determination
that the requestor is a trusted requestor.

5   16.   The data processing system of claim 15, wherein the
bus system includes a primary bus and a secondary bus.

17.   The data processing system of claim 15, wherein the
processor unit includes a single processor.

10

18.   The data processing system of claim 15, wherein the
processor unit includes a plurality of processors.

19.   The data processing system claim 15, wherein the
15   communications unit is an Ethernet adapter.

20.   A data processing system for managing access to data
in a datastore, the data processing system comprising:
        receiving means for receiving a request for access
20   to an item of data from a requestor, wherein the item of
data is encrypted using a key;
        determining means for determining whether the
requestor is a trusted requestor; and
        decrypting means, responsive to a determination that
25   the requestor is a trusted requestor, for decrypting the
item of data using the key to form a decrypted item of
data; and
        sending means for sending the decrypted item of data
to the requestor.

30

21.   The data processing system of claim 20, wherein the

Docket No.   AUS920000797US1

requestor is an application.

22.   The data processing system of claim 20, wherein the Keystore is a Java Keystore.

5

23.   The data processing system of claim 20, wherein the item of data is another key.

24.   The data processing system of claim 20, wherein the
10   item of data is a certificate.

25.   The data processing system of claim 20, wherein the item of data is indexed within the Keystore using an alias.

15

26.   The data processing system claim 25, wherein the request includes the alias further comprising:

returning means, responsive to an absence of a determination that the requestor is a trusted requestor,
20   for returning a null result to the requestor.

27.   The data processing system of claim 20 further comprising:

encrypting means, responsive to receiving a request
25   to add a new item of data to the Keystore, for encrypting the new item of data to form an encrypted item of data; and

storing means for storing the encrypted item of data in the Keystore.

30

28.   The data processing system of claim 27, wherein the

Docket No.   AUS920000797US1

storing means is a first storing means further
comprising:

        second storing means for storing the new item of
data in the Keystore.

5

29.   The data processing system of claim 27, wherein
each item of data in the Keystore is associated with an
alias.

10   30.   A data processing system for managing access to data
in a datastore, the data processing system comprising:
        receiving means for receiving a request for access
to an item of data from a requestor, wherein the item of
data is encrypted using a key;
15   determining means for determining whether the
requestor is a trusted requestor; and
        sending means, responsive to a determination that
the requestor is a trusted requestor, for sending the key
and the item of data to the requestor.
20

31.   A computer program product in a computer readable
medium for managing access to data in a datastore, the
computer program product comprising:
        first instructions for receiving a request for
25   access to an item of data from a requestor, wherein the
item of data is encrypted using a key;
        second instructions for determining whether the
requestor is a trusted requestor; and
        third instructions, responsive to a determination
30   that the requestor is a trusted requestor, for sending
the key and the item of data to the requestor.

Docket No.   AUS920000797US1

32.   A computer program product in a computer readable
medium for managing access to data in a datastore, the
computer program product comprising:

5   first instructions for receiving a request for
access to an item of data from a requestor, wherein the
item of data is encrypted using a key;

         second instructions for determining whether the
requestor is a trusted requestor;

10   third instruction, responsive to a determination
that the requestor is a trusted requestor, for decrypting
the item of data using the key to form a decrypted item
of data; and

         fourth instructions for sending the decrypted item
15 of data to the requestor.